BỘ TÀI CHÍNH **TỔNG CỤC HẢI QUAN**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 1728 /QĐ-TCHQ	*Hà Nội, ngày 18 tháng 6 năm 2019*

QUYẾT ĐỊNH
Về việc ban hành "Kiến trúc và khung tiêu chuẩn an toàn bảo mật hệ thống công nghệ thông tin ngành Hải quan"

TỔNG CỤC TRƯỞNG TỔNG CỤC HẢI QUAN

Căn cứ Luật An toàn thông tin mạng năm 2015;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Quyết định số 65/2015/QĐ-TTg ngày 17/12/2015 của Thủ tướng Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Tổng cục Hải quan trực thuộc Bộ Tài chính;

Căn cứ Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Quyết định số 2582/QĐ-BKHCN ngày 25/9/2017 của Bộ trưởng Bộ Khoa học và Công nghệ về việc công bố Tiêu chuẩn quốc gia TCVN 11930:2017 yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ;

Căn cứ Quyết định 201/QĐ-BTC ngày 12/02/2018 của Bộ trưởng Bộ Tài chính ban hành Quy chế An toàn thông tin mạng Bộ Tài chính;

Căn cứ Quyết định 2445/QĐ-BTC ngày 28/12/2018 của Bộ trưởng Bộ Tài chính ban hành Kiến trúc Chính phủ điện tử ngành Tài chính;

Căn cứ Công văn 1178/BTTTT-THH ngày 21/4/2015 của Bộ Thông tin và Truyền thông ban hành Khung Kiến trúc chính phủ điện tử Việt Nam phiên bản 1.0;

Xét đề nghị của Cục trưởng Cục Công nghệ thông tin & Thống kê Hải quan,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này "Kiến trúc và khung tiêu chuẩn an toàn bảo mật hệ thống công nghệ thông tin ngành Hải quan".

Điều 2. Kiến trúc và khung tiêu chuẩn an toàn bảo mật hệ thống công nghệ thông tin ngành Hải quan làm căn cứ để xây dựng, triển khai, tổ chức thực hiện các giải pháp nhằm đảm bảo an toàn thông tin cho hệ thống thông tin ngành Hải quan.

Điều 3. Quyết định này có hiệu lực kể từ ngày ký. Cục trưởng Cục CNTT&Thống kê Hải quan, Thủ trưởng các đơn vị thuộc, trực thuộc Tổng cục Hải quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Bộ Tài chính (để báo cáo);
- Lưu: VT, CNTT (5b).

KT. TỔNG CỤC TRƯỞNG
PHÓ TỔNG CỤC TRƯỞNG

BỘ TÀI CHÍNH TỔNG CỤC HẢI QUAN

Nguyễn Công Bình

BỘ TÀI CHÍNH
TỔNG CỤC HẢI QUAN

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

QUY ĐỊNH
Kiến trúc và khung tiêu chuẩn an toàn bảo mật hệ thống công nghệ thông tin ngành Hải quan

(Ban hành kèm Quyết định số 1728/QĐ-TCHQ ngày 18 tháng 6 năm 2019 của Tổng cục trưởng Tổng cục Hải quan)

1. Mục đích

Nâng cao mức độ an ninh an toàn thông tin cho hệ thống công nghệ thông tin ngành Hải quan;

Làm cơ sở để xây dựng, triển khai, quản lý các giải pháp đảm bảo an toàn thông tin cho các hệ thống Công nghệ thông tin (CNTT) trong ngành Hải quan theo một kiến trúc, tiêu chuẩn thống nhất.

2. Kiến trúc an toàn bảo mật hệ thống công nghệ thông tin ngành Hải quan

2.1. Mô hình kiến trúc:

Khung Kiến trúc an toàn bảo mật hệ thống công nghệ thông tin ngành Hải quan thực hiện: Xác định các đối tượng cần được bảo vệ và các giải pháp, hoạt động về an toàn thông tin (ATTT) phải thực hiện để bảo vệ đối tượng đó. Cụ thể:

- Chiều dọc: Xác định các đối tượng cần bảo vệ gồm: Thiết bị người dùng cuối (PC, Laptop), Thiết bị Phòng máy chủ, Trung tâm dữ liệu (Server, Appliance, Cloud), Hạ tầng mạng (Mạng nội bộ, WAN, Internet), Hệ thống ứng dụng & dịch vụ (Email, Database, Ứng dụng nội bộ, Ứng dụng cung cấp ra ngoài, Trang tin portal).
- Chiều ngang: Xác định các giải pháp, hoạt động để thực thi hiệu quả chiến lược ATTT nhằm bảo vệ các đối tượng trong hệ thống công nghệ thông tin ngành Hải quan; gồm 3 nhóm hành động chính:
    - Phòng ngừa, bảo vệ ;
    - Giám sát, phát hiện, ứng cứu và xử lý sự cố ;
    - Quản lý nhân lực, mô hình tổ chức bộ phận ATTT.

<table>
<tr><th colspan="10">KHUNG KIẾN TRÚC AN TOÀN BẢO MẬT</th></tr>
<tr><td rowspan="2">Đối tượng

Giải pháp</td><td rowspan="2">Thiết bị người dùng (PC, Laptop)</td><td rowspan="2">Thiết bị Phòng máy chủ, Trung tâm dữ liệu (Servers, Appliance, Cloud)</td><td colspan="3">Hạ tầng mạng</td><td colspan="5">Ứng dụng và dịch vụ</td></tr>
<tr><td>Mạng nội bộ (LAN)</td><td>Mạng diện rộng (WAN)</td><td>Mạng Internet</td><td>Thư điện tử (Email)</td><td>Cơ sở dữ liệu</td><td>Ứng dụng nội bộ</td><td>Ứng dụng cung cấp dịch vụ ra ngoài</td><td>Trang tin (Portal)</td></tr>
<tr><td colspan="10">Phòng ngừa, bảo vệ</td></tr>
<tr><td rowspan="3">Giải pháp kỹ thuật</td><td colspan="4">An toàn vật lý
(Physical Security)</td><td>Chống Spam
(AntiSpam)</td><td>Tường lửa CSDL
(DB Firewall)</td><td colspan="3">Tường lửa ứng dụng web
(Web Application Firewall)</td></tr>
<tr><td colspan="3">Phần mềm diệt virus
(AV)</td><td colspan="2">Tường lửa
(Firewall)</td><td>Phòng chông virus cho email
(Mail AV)</td><td colspan="2">Bảo mật dữ liệu
(Data Security)</td><td colspan="2">Chống tấn công DDOS lớp ứng dụng
(Anti DDoS L7)</td></tr>
<tr><td>Hệ thống quản lý người dùng tập trung
(Domain Controller)</td><td>Phòng chống tấn công lớp máy chủ
(Host IPS)</td><td colspan="2">Phòng chống tấn công lớp mạng
(Network IPS)</td><td>Chống tấn công APT cho email
(Mail Anti-APT)</td><td colspan="4"></td></tr>
</table>

	Chống tấn công APT thiết bị người dùng **(Enpoint Anti-APT)**	Chống tấn công APT máy chủ **(Server Anti-APT)**	Chống tấn công APT lớp mạng **(Network Anti APT)**		
	Quản lý bản vá **(Patch management)**		Quản lý, giám sát mạng **(Network Management)**		
	Bảo mật dữ liệu **(Data Security)**	Quản lý tài khoản đặc quyền **(PIM)**		Mạng riêng ảo **(VPN)**	
				Proxy	
				Chống tấn công DDOS tràn băng thông **(Anti-DdoS Volume Based)**	

<table>
<tr><td>Quy chế, quy định, tiêu chuẩn ATTT</td><td colspan="4">Hệ thống chính sách (Quy chế, quy trình, tiêu chuẩn ATTT) cho thiết bị người dùng, máy chủ, mạng, ứng dụng, dịch vụ (Áp dụng các tiêu chuẩn TCVN, ISO 27000, NIST,…)</td></tr>
<tr><td>Thiết kế và triển khai chính sách ATTT</td><td colspan="4">Thiết kế mô hình mạng chuẩn và triển khai các tiêu chuẩn ATTT</td></tr>
<tr><td rowspan="2">Sao lưu và phục hồi</td><td colspan="4">Sao lưu tự động hoặc định kỳ (Cấu hình, CSDL, mã nguồn, …).</td></tr>
<tr><td colspan="4">Diễn tập khôi phục hệ thống từ bản sao lưu</td></tr>
<tr><td>Rà soát, đánh giá bảo mật</td><td colspan="4">Rà soát đánh giá bảo mật cho: hạ tầng mạng, máy chủ, ứng dụng, thiết bị phòng máy chủ, máy tính người dùng, ….</td></tr>
<tr><td>Đào tạo</td><td colspan="4">Đào tạo kiến thức bảo mật phù hợp với từng đối tượng: Nhân viên, lập trình viên, quản trị hệ thống, chuyên viên ATTT, lãnh đạo</td></tr>
<tr><td colspan="5">Giám sát phát hiện, ứng cứu, xử lý sự cố</td></tr>
<tr><td rowspan="2">Triển khai các công cụ hỗ trợ quản lý, giám sát phát hiện vi phạm, nguy cơ ATTT</td><td colspan="4">Hệ thống quản lý các sự kiện ATTT
SIEM (Security Information Event Management)</td></tr>
<tr><td>Giám sát ATTT máy tính người dùng (Endpoint Security Baseline Monitoring)</td><td>Giám sát ATTT máy chủ (Server Security Baseline Monitoring)</td><td>Giám sát ATTT lớp mạng (Network Security Baseline Monitoring)</td><td>Quản thông tin ứng dụng, dịch vụ, cấu hình, cài đặt (Application profilling)</td></tr>
</table>

<table>
<tr><td rowspan="2"></td><td>Phát hiện bất thường trên máy tính người dùng (Endpoint Anomaly Detection)</td><td>Phát hiện bất thường trên máy chủ (Server Anomaly Detection)</td><td colspan="2">Phát hiện bất thường lớp mạng (Network Anomaly Detection)</td><td colspan="2"></td><td>Giám sát thư mục ứng dụng (Directory Monitoring)</td></tr>
<tr><td colspan="2"></td><td>Điều khiển truy cập mạng (NAC)</td><td colspan="4"></td></tr>
<tr><td rowspan="2">Dự đoán, phát hiện sớm các nguy cơ ATTT</td><td colspan="7">Rà soát, truy vết phát hiện các nguy cơ ATTT
(Threat Hunting)</td></tr>
<tr><td>Cập nhật các thông tin nguy cơ ATTT (Threat Intelligence)</td><td colspan="6">Phân tích các sự kiện ATTT dựa trên phân tích dữ liệu lớn, khai phá dữ liệu
(Security Event Datamining & Big data analytic)</td></tr>
<tr><td rowspan="2">Giám sát ATTT 24/07 (Tier 1)</td><td colspan="7">Triển khai hệ thống công cụ, thiết bị hạ tầng, văn phòng hỗ trợ giám sát ATTT
(Monitoring System)</td></tr>
<tr><td colspan="7">Triển khai giải pháp hỗ trợ quản lý cảnh báo, theo vết, xử lý toàn diện các cảnh báo ATTT
(Security Management)</td></tr>
</table>

	Quy trình, hướng dẫn giám sát, xử lý cảnh báo ATTT **(SOC processes & Reponse Guideline)**
	Tổ chức nhân sự trực giám sát ATTT 24/7 **(Tier 1 Security Monitoring 24/7)**
Xử lý sự cố (Tier 2)	Hệ thống quản lý ticket xử lý sự cố **(Incident Ticket Management System)**
	Quy trình, hướng dẫn xử lý sự cố ATTT **(SOC Processes & Escalation Guideline)**
	Xử lý chấm dứt sự cố, khắc phục các nguyên nhân gây ra sự cố **(Incident Resolve)**
Điều tra, xử lý sự cố mức chuyên gia (Tier 3)	Điều tra, truy vết, xác định nguyên nhân, nguồn gốc, thủ phạm tấn công **(Investigation)**
	Xử lý các sự cố mới, sự cố diện rộng với chuyên gia mức cao **(Processing Security Expert Level)**
Diễn tập xử lý sự cố	Tổ chức diễn tập xử lý sự cố ATTT
Quản lý nhân sự, mô hình tổ chức bộ phận ATTT	
Quản lý nhân sự ATTT	Bộ máy, nhân sự ATTT Lãnh đạo cấp cao phụ trách ATTT (CIO)

2.2. Các thành phần thuộc kiến trúc:

a. Công tác phòng ngừa, bảo vệ:

- **Triển khai các giải pháp bảo vệ**:
    - Thiết bị người dùng cuối (PC, Laptop): Phần mềm AntiVirus, Hệ thống quản lý người dùng tập trung, Giải pháp chống tấn công APT máy tính người dùng, Hệ thống quản lý bản vá lỗ hổng, Giải pháp bảo mật dữ liệu trên máy tính người dùng.
    - Phòng máy chủ, Trung tâm dữ liệu (Server, Appliance, Cloud, ...): Phần mềm diệt virus cho máy chủ, Phần mềm chống tấn công lớp máy chủ (Host IPS), Giải pháp chống tấn công APT máy chủ, Hệ thống quản lý bản vá, Hệ thống quản lý đặc quyền.
    - Hạ tầng mạng (LAN, WAN, Internet): Thiết bị tường lửa, Thiết bị phát hiện tấn công lớp mạng, Giải pháp chống tấn công APT lớp mạng, Hệ thống giám sát, quản lý lớp mạng, Mạng riêng ảo VPN, Cổng kết nối Internet Proxy, Giải pháp chống tấn công DDOS tràn băng thông.
    - Ứng dụng, dịch vụ (Email, Cơ sở dữ liệu, Ứng dụng nội bộ, Ứng dụng dịch vụ cung cấp bên ngoài, trang tin Portal): Antispam, Diệt virus cho mail, Chống tấn công APT cho email, Tường lửa CSDL, Giải pháp bảo mật dữ liệu, Tường lửa ứng dụng web, chống tấn công DDOS lớp ứng dụng;
- **Xây dựng hệ thống quy định, chính sách về an toàn thông tin**: Là cơ sở duy trì hoạt động, vận hành đảm bảo tính an toàn an ninh thông tin cho hệ thống CNTT diễn ra liên tục. Hệ thống chính sách ATTT được xây dựng dựa trên các chuẩn quốc tế như ISO 27000, NIST và các quy định của nhà nước.
- **Thiết kế, quy hoạch, triển khai hệ thống đảm bảo an toàn thông tin**: quy hoạch chuẩn hóa hệ thống mạng, cấu hình đảm bảo an toàn thông tin cho các hệ thống, ứng dụng, dịch vụ.
- **Sao lưu và phục hồi**: hoạt động phòng ngừa chuẩn bị khả năng phục hồi lại hệ thống khi có sự cố, bao gồm 2 hành động chính cần thực hiện:
    - Tiến hành sao lưu tự động hoặc định kỳ tất cả các thông tin hỗ trợ khôi phục lại hệ thống như cấu hình, cơ sở dữ liệu, mã nguồn, ...
    - Diễn tập khôi phục sự cố từ bản sao lưu: Đảm bảo hoạt động sao lưu diễn ra bình thường, dữ liệu sao lưu cập nhật, đủ khả năng khôi phục lại hệ thống thực sự, tránh bị động khi xảy ra sự cố.
- **Đánh giá, phát hiện, khắc phục các lỗ hổng, nguy cơ của hệ thống**: chủ động rà soát, đánh giá các hệ thống phát hiện các lỗ hổng, nguy cơ về an toàn thông tin để thực hiện khắc phục, đảm bảo ATTT cho hệ thống. Hoạt động đánh giá được áp dụng cho tất cả các đối tượng trong hệ thống CNTT. Thực

hiện qua 2 hình thức: Tấn công khai thác thử nghiệm và Đánh giá rà soát toàn diện. Việc thực hiện đánh giá phải đảm bảo tính độc lập giữa hoạt động đánh giá và hoạt động vận hành khai thác, phát triển hệ thống để đảm bảo tính khách quan cũng như cung cấp nhiều góc nhìn về hệ thống.

- **Đào tạo**: Đảm bảo nhận thức đúng về nguy cơ, cách làm an toàn thông tin. Đồng thời, thường xuyên đào tạo lực lượng chuyên môn cập nhật các công nghệ, tiêu chuẩn ATTT.

b. Giám sát, phát hiện, ứng cứu, xử lý sự cố:

- **Triển khai các công cụ hỗ trợ quản lý, giám sát phát hiện vi phạm, nguy cơ ATTT**: triển khai các công cụ, giải pháp nhằm xác định các thông tin chuẩn hóa ở trạng thái bình thường của các hệ thống, đối tương, ứng dụng; là thông tin cơ sở để xác định bất thường. Việc thực hiện quản lý được thực hiện thông qua các công cụ như: Các giải pháp quản lý thông tin, trạng thái các thành phần trong hệ thống CNTT; Hệ thống quản lý các sự kiện - SIEM, Giải pháp giám sát tiêu chuẩn ATTT lớp người dùng, máy chủ, lớp mạng; Giải pháp quản lý thông tin ứng dụng, dịch vụ, cấu hình, cài đặt các hệ thống ứng dụng; Giải pháp phát hiện bất thường trên máy người dùng, máy chủ, lớp mạng; Giải pháp giám sát thư mục ứng dụng; Giải pháp quản lý điều khiển truy cập mạng NAC.
- **Dự đoán, phát hiện sớm các mối đe dọa về an toàn thông tin**: Dựa trên phân tích các thông tin về tình trạng tấn công mạng trên thế giới, ở Việt Nam nhằm phân tích các dấu hiệu, các nguồn dữ liệu, nhận dạng các chuỗi sự kiện bất thường phát hiện các dạng tấn công dai dẳng, ẩn náu trong hệ thống.
- **Giám sát ATTT 24/7**: Giám sát, phát hiện các dấu hiệu sự cố, tấn công, vi phạm các tiêu chuẩn cấu hình ATTT của hệ thống. Bao gồm các hành động chính sau:
    - Triển khai các hệ thống công cụ, thiết bị hạ tầng, văn phòng, cơ sở vật chất hỗ trợ việc trực giám sát 24/7 như: máy tính, màn hình giám sát, điện thoại, văn phòng, chỗ làm việc đảm bảo hỗ trợ cho nhân viên trực 24/7.
    - Triển khai giải pháp hỗ trợ quản lý cảnh báo, theo vết, xử lý toàn diện các cảnh báo ATTT: Hệ thống quản lý các cảnh báo ATTT tập trung, cho phép xử lý, tạo ticket, gán, chuyển công việc xử lý đến các bộ phận vận hành, phát triển các hệ thống Công nghệ thông tin.
    - Xây dựng hệ thống quy trình, hướng dẫn giám sát, KPI xử lý cảnh báo ATTT.
    - Tổ chức nhân sự trực giám sát ATTT 24/7 theo ca, kíp trực đảm bảo trực 24/7 tất cả các ngày trong năm.

- **Xử lý sự cố (Tier 2)**: Để xử lý kịp thời, khép kín các sự cố ATTT, cần thực hiện các hành động chính sau:
    - Triển khai hệ thống quản lý ticket sự cố ATTT: Hệ thống cho phép quản lý, luân chuyển, chia tách công việc thành các công việc chi tiết, đảm bảo sự cố được xử lý triệt để, với đầy đủ luồng, lưu vết lịch sử xử lý.
    - Xây dựng hệ thống quy trình, hướng dẫn xử lý sự cố ATTT triệt để.
    - Xử lý chấm dứt sự cố, khắc phục các nguyên nhân gốc gây ra sự cố.
- **Điều tra, xử lý sự cố mức chuyên gia (Tier 3):** bao gồm 2 hoạt động chính:
    - Điều tra (Investigation): Điều tra, xác định nguyên nhân sự cố, phương thức, hành động tấn công, và cả thủ phạm tấn công vào hệ thống.
    - Xử lý sự cố bởi chuyên gia: Với các sự cố ATTT phức tạp, xử lý mức chuyên gia là yêu cầu bắt buộc, bởi hành động, phương thức tấn công, kỹ thuật tấn công là yếu tố không xác định trước, rất khó xác định nếu thiếu kiến thức chuyên môn sâu.
- **Diễn tập xử lý sự cố**: Nhằm sẵn sàng cho mọi tình huống xảy ra khi sự cố với đầy đủ các kịch bản tấn công.

c. Quản lý nhân sự, mô hình tổ chức bộ phận ATTT:

- Định hình vị trí, vai trò chức danh CIO, CSO
- Các định hướng, chiến lược, tổ chức về nhân lực ATTT trong tổ chức.

3. Khung tiêu chuẩn an toàn bảo mật hệ thống công nghệ thông tin ngành Hải quan

3.1. Mô hình khung tiêu chuẩn:

Hệ thống CNTT phân theo cấp độ														
An toàn vật lý cho hệ thống CNTT						An toàn hệ thống CNTT								
						Yêu cầu quản lý					Yêu cầu kỹ thuật			
Vị trí vật lý	Kiểm soát truy cập vật lý, chống trộm	Chống sét, chống tĩnh điện	Chống cháy	Kiểm soát nhiệt độ, độ ẩm	Nguồn cấp, bảo vệ điện từ	Thiết lập chính sách ATTT	Tổ chức đảm bảo ATTT	Đảm bảo nguồn nhân lực	Quản lý thiết kế, xây dựng hệ thống	Quản lý vận hành hệ thống	Bảo đảm an toàn mạng	Bảo đảm an toàn máy chủ	Bảo đảm an toàn ứng dụng	Bảo đảm an toàn dữ liệu

3.2. Nội dung khung tiêu chuẩn:

a. Hệ thống CNTT phân theo cấp độ:

Tiêu chí xác định cấp độ, thẩm quyền, trình tự, thủ tục xác định cấp độ thực hiện theo Nghị định 85/2016/NĐ-CP ngày 01/7/2016, Thông tư 03/2017/TT-BTTTT ngày 24/4/2017 và Quyết định số 201/QĐ-BTC ngày 12/02/2018;

b. Tiêu chuẩn An toàn vật lý cho hệ thống CNTT Hải quan:

Tiêu chuẩn An toàn vật lý cho hệ thống CNTT Hải quan thực hiện theo hướng dẫn tại Tiêu chuẩn quốc gia TCVN 11930:2017 - yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ và Tiêu chuẩn hạ tầng kỹ thuật phòng máy chủ ngành Hải quan đã được ban hành;

c. Tiêu chuẩn An toàn cho hệ thống thông tin:

Tiêu chuẩn An toàn vật lý cho hệ thống CNTT Hải quan thực hiện theo hướng dẫn tại Tiêu chuẩn quốc gia TCVN 11930:2017 - yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ;

4. Tổ chức thực hiện

4.1. Cục Công nghệ thông tin và Thống kê Hải quan:

- Chịu trách nhiệm chính trong việc cập nhật, duy trì và tổ chức triển khai "Kiến trúc và khung tiêu chuẩn an toàn bảo mật hệ thống công nghệ thông tin ngành Hải quan" trong ngành Hải quan;
- Hướng dẫn, kiểm tra tính tuân thủ của các đơn vị trong việc triển khai "Kiến trúc và khung tiêu chuẩn an toàn bảo mật hệ thống công nghệ thông tin ngành Hải quan".

4.2. Các đơn vị thuộc, trực thuộc Tổng cục Hải quan:

- Xây dựng kế hoạch ứng dụng công nghệ thông tin hàng năm theo phân cấp đảm bảo tuân thủ "Kiến trúc và khung tiêu chuẩn an toàn bảo mật hệ thống công nghệ thông tin ngành Hải quan";
- Phối hợp với Cục Công nghệ thông tin và Thống kê Hải quan xây dựng, triển khai các hệ thống công nghệ thông tin phù hợp với "Kiến trúc và khung tiêu chuẩn an toàn bảo mật hệ thống công nghệ thông tin ngành Hải quan".

5. Lộ trình thực hiện

5.1. ***Giai đoạn tới năm 2020***

- Từng bước hoàn thiện các giải pháp phòng ngừa bảo vệ bảo đảm an ninh an toàn cho hệ thống CNTT Hải quan: Bổ sung, hoàn thiện các giải pháp kỹ thuật bảo đảm an ninh an toàn cho các đối tượng cần bảo vệ tại Trung tâm dữ liệu Tổng cục Hải quan, phòng máy chủ các Cục Hải quan; Ban hành quy chế an toàn thông tin mạng Tổng cục Hải quan nhằm thay thế Quy chế đảm bảo an ninh, an toàn hệ thống công nghệ thông tin Hải quan ban hành tại Quyết định 2926/QĐ-TCHQ ngày 06/10/2014; Xác định cấp độ cho hệ thống thông tin đủ điều kiện; Rà soát, đánh giá bảo mật cho hệ thống công nghệ thông tin; Tiếp tục đào tạo nâng cao trình độ cho đội ngũ làm công tác quản trị, an ninh an toàn.
- Thuê dịch vụ triển khai trung tâm giám sát an toàn thông tin mạng (SOC) nhằm giám sát phát hiện, ứng cứu và xử lý các sự cố an toàn thông tin cho hệ thống thông tin Hải quan.
- Định kỳ tổ chức diễn tập xử lý sự cố An toàn thông tin.

5.2. ***Giai đoạn 2021 – 2025***

- Tiếp tục hoàn thiện các giải pháp phòng ngừa bảo vệ bảo đảm an ninh an toàn cho hệ thống CNTT Hải quan: Hoàn thiện các giải pháp kỹ thuật bảo đảm an ninh an toàn; Hoàn thiện các quy chế, quy trình, tiêu chuẩn ATTT trong ngành Hải quan phù hợp với các quy định của pháp luật, của ngành; Xác định cấp độ cho hệ thống thông tin; Đào tạo xây dựng đội ngũ chuyên gia về ATTT, đào tạo nâng cao nhận thức về ATTT cho người sử dụng.
- Kết nối trung tâm giám sát an toàn thông tin mạng (SOC) ngành Hải quan

với SOC ngành Tài chính.

- Định kỳ rà soát, đánh giá bảo mật cho hệ thống công nghệ thông tin; diễn tập xử lý sự cố An toàn thông tin.
- Kiện toàn bộ máy, nhân sự ATTT theo vị trí, chức danh công việc./.

KT. TỔNG CỤC TRƯỞNG
PHÓ TỔNG CỤC TRƯỞNG

BỘ TÀI CHÍNH
TỔNG CỤC HẢI QUAN

Nguyễn Công Bình